MA441: Algebraic Structures I

Lecture 7

24 September 2003

Review from Lecture 6:

Theorem 4.1: Criterion for $a^i = a^j$

Let G be a group, and let a belong to G. If a has infinite order, then all distinct powers of a are distinct group elements. If a has finite order, say, n, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and $a^i = a^j$ if and only if n divides $i - j$.

Corollary 1:
For any group element a,

$$|a| = |\langle a \rangle|.$$

Corollary 2:
Let G be a group and let $a \in G$ have order n. If $a^k = e$, then n divides k.

Theorem 4.2:

Let a be an element of order n in a group and let k be a positive integer. Then

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$$

and

$$|a^k| = \frac{n}{\gcd(n,k)}.$$

Corollary 1:
Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n,i) = \gcd(n,j)$.

Proof:
By Theorem 4.2, we have that $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$.

We need to prove $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ iff $\gcd(n,i) = \gcd(n,j)$.

Clearly $\gcd(n,i) = \gcd(n,j)$ implies $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$.

Suppose that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$.

This means $|\langle a^{\gcd(n,i)} \rangle| = |\langle a^{\gcd(n,j)} \rangle|$, so $|a^{\gcd(n,i)}| = |a^{\gcd(n,j)}|$.

By the second part of Theorem 4.2, on the LHS $|a^{\gcd(n,i)}| = n/\gcd(n,i)$ and on the RHS $|a^{\gcd(n,j)}| = n/\gcd(n,j)$. Therefore,

$$\frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)},$$

so $\gcd(n,i) = \gcd(n,j)$.

Here are two special cases of Corollary 1.

Corollary 2:
Let $G = \langle a \rangle$ be a cyclic group of order n. Then $G = \langle a^k \rangle$ iff $\gcd(n, k) = 1$.

Corollary 3:
An integer k in $\mathbb{Z}/n\mathbb{Z}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(n, k) = 1$.

(Compare this to exercises 1, 2 of Chapter 4.)

Classification of Subgroups of Cyclic Groups

(From Chapter 4, page 78)

Theorem 4.3: Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely, $\langle a^{n/k} \rangle$.

Example:
What are the subgroups of a cyclic group $\langle a \rangle$ of order 30?

Consider the divisors of 30: $\{1, 2, 3, 5, 6, 10, 15, 30\}$.

Corollary: Subgroups of $\mathbb{Z}/n\mathbb{Z}$

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order k; moreover, these are the only subgroups of $\mathbb{Z}/n\mathbb{Z}$.

Proof of Theorem 4.3:

Claim 1:
Every subgroup of a cyclic group is cyclic.

Let $G = \langle a \rangle$ and suppose $H \leq G$. We must show H is cyclic.

If H is the trivial subgroup, i.e., $H = \{e\}$, then it is cyclic. So assume H is nontrivial, i.e., $H \neq \{e\}$.

H contains an element a^t for some $t > 0$.

(Why?)

Since $H \leq G = \langle a \rangle$, there is some power of a in H, say, a^t. If $t < 0$, then the inverse of a^t, a^{-t} is in H and $-t > 0$.

Let m be the least positive integer such that $a^m \in H$.

By closure, $\langle a^m \rangle \subseteq H$.

Because we have chosen m to be the least power of a in H, by using the division algorithm, we can show that $\langle a^m \rangle \supseteq H$.

(Why?)

Let b be any element of H. Since $H \leq \langle a \rangle$, $b = a^k$ for some k. Since m is least, $m \leq k$.

Apply the division algorithm to k and m to divide k by m and get a quotient q with remainder r such that $0 \leq r < m$:

$$k = mq + r,$$

hence

$$a^k = a^{mq} \cdot a^r.$$

How can we write a^r in terms of a^k and a^m?

Compute $a^r = a^k \cdot (a^m)^{-q}$. $(r = k - mq)$

What can we conclude about r?

Since 0 $\leq r < m$, yet m is the least positive integer such that $a^m \in H$, we must have

$$r = 0.$$

What does this tell us about our arbitrary $b \in H$?

What about the relationship between H and $\langle a^m \rangle$?

Since $b = a^k$, $r = 0$, therefore $k = mq$ and

$$b = a^k = (a^m)^q,$$

so $b \in \langle a^m \rangle$.

Then $H \subseteq \langle a^m \rangle$, which gives us

$$H = \langle a^m \rangle.$$